(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
31. Mai 2001 (31.05.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/38954 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00, H04L 29/06

(21) Internationales Aktenzeichen: PCT/EP00/09428

(22) Internationales Anmeldedatum:
27. September 2000 (27.09.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 57 467.7 24. November 1999 (24.11.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **ALTHOFF, Jürgen** [DE/DE]; Fritz-Erler-Str. 5, 48429 Rheine (DE). **DOMEYER, Stefan** [DE/DE]; Berliner Str. 84, 38104 Braunschweig (DE).

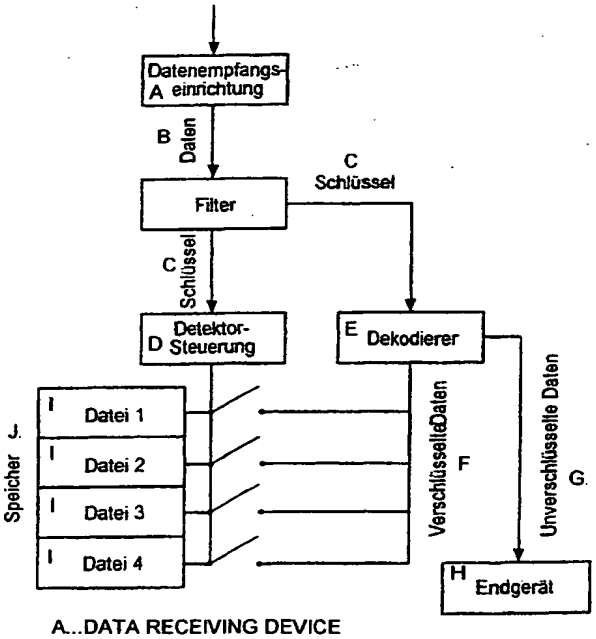
(74) Gemeinsamer Vertreter: **DEUTSCHE TELEKOM AG**; Rechtsabteilung (Patente) PA1, 64307 Darmstadt (DE).

(81) Bestimmungsstaaten *(national)*: BR, IL, IN, JP, PL, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR USING ENCRYPTED DATA

(54) Bezeichnung: VERFAHREN ZUR ANWENDUNG VERSCHLÜSSELTER DATEN



A...DATA RECEIVING DEVICE
B...DATA
C...CODE
D...DETECTOR CONTROL
E...DECODER
F...ENCRYPTED DATA
G...UNENCRIPTED DATA
H...TERMINAL
I...FILE
J...MEMORY

(57) **Abstract:** The transmission of large data quantities is complicated by limited transmission capacities. In the case of encrypted data, the codes must also be transmitted. The invention provides a method in which the encrypted data is stored on media which can be physically sent to the user. Only the codes are transmitted to the users via a telecommunications network and can be specifically addressed or addressed in universally accessible manner. Said codes reach the users, according to a transmittal plan or when the users retrieve them, where they exclusively permit access to the encrypted data during the period of availability, and they cannot be stored. Different codes are also used in the case of different contents contained on the storage media. The accessibility by using codes can be centrally recorded.

(57) **Zusammenfassung:** Die Übertragung grosser Datenmengen wird erschwert durch begrenzte Übertragungskapazitäten. Bei verschlüsselten Daten müssen zusätzlich die Schlüssel übertragen werden. Mit der vorliegenden Erfindung wird ein Verfahren angeboten, bei dem die verschlüsselten Daten auf Medien gespeichert werden, die physisch an die Nutzer verschickt werden können. Über ein Telekommunikationsnetz werden lediglich die Schlüssel zu den Nutzern übertragen und können allgemein zugänglich oder speziell adressiert, nach einem Sendeplan oder auf Abruf die Nutzer erreichen, wo sie ausschliesslich während der Zeitdauer der Verfügbarkeit den Zugang zu den verschlüsselten Daten ermöglichen und nicht gespeichert werden können. Bei unterschiedlichen Inhalten auf den Speichermedien werden auch unterschiedliche Schlüssel verwendet. Die Zugriffsmöglichkeit über die Schlüssel kann zentral erfasst werden.

WO 01/38954 A1

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren zur Anwendung verschlüsselter Daten

Beschreibung

Die Erfindung betrifft die Anwendung verschlüsselter Daten sowie die Bedingungen für den Zugriff auf die Daten.

Bei großen Datenmengen ist die begrenzte Übertragungskapazität ein Problem, soweit die Daten einzeln abgerufen und bezahlt werden sollen.

Stand der Technik

Nach dem Stand der Technik ermöglichen Datenbanksysteme einen Zugriff auf Daten in der Weise, dass die Daten in Reaktion auf eine Anforderung hin an den Nutzer übertragen werden. Die Daten können dabei sowohl verschlüsselt, als auch unverschlüsselt sein. Der Zugriff kann lokal oder aus der Ferne erfolgen.

Als Zugriffssysteme sind bekannt:
Client-server-Konfigurationen in LAN und WAN, DFÜ-Fest- oder Wählverbindungen, Conditional-Access-Systeme (Zugangskontrollsysteme) bei funkgestützter Datenübertragung.

Vorteile und Unterscheidungsmerkmale der Erfindung gegenüber dem Stand der Technik

Es wird unterschieden zwischen verschlüsselten Daten und Schlüsseln. Die Daten, die in der Regel sehr umfangreich sind, werden auf einem Speichermedium (z. B. DVD-ROM, CD-ROM) physisch zum Anwender transportiert. Die Schlüssel werden über ein Datennetz

Datenfluss zwischen Speichermedium und Dekodierer unterbrochen – etwa weil der Schlüssel nicht mehr gesendet wird – so kann der Nutzer keinen Zugriff mehr auf die Daten nehmen.

Bezugszeichen-Auflistung

LAN	Local Area Network
WAN	Wide Area Network
DFÜ	Daten-Fern-Übertragung
DVD	Digital Versatile Disc
CD	Compact Dis
ROM	Read Only Memory
ISDN	Integrated Services Digital Network
BOT	Broadcast Online Television
GSM	Global System for Mobile communication

Patentansprüche (3)

1. Verfahren zur Anwendung verschlüsselter Daten, d a d u r c h g e k e n n z e i c h n e t, dass die verschlüsselten Daten auf Speichermedien gespeichert werden, die an die Nutzer physisch versendet werden können,
dass die Schlüssel zur Entschlüsselung der Daten über ein Datennetz übertragen werden,
dass die Schlüssel von allen Netzteilnehmern zu empfangen sind oder alternativ nur einzelne Nutzer bzw. Nutzergruppen adressiert werden können,
dass der Versand der Schlüssel sowohl nach einem im Voraus festgelegten Sendeplan als auch auf Abruf durch die Nutzer erfolgen kann,
dass die gesendeten Schlüssel zum Zeitpunkt des Eintreffens beim Nutzer unmittelbar verarbeitet werden und nicht gespeichert werden können,
dass der Zugriff auf die verschlüsselten Daten zeitlich bestimmt wird durch die Verfügbarkeit der empfangenen Schlüssel, und
dass der Empfang der Schlüssel an weitere Bedingungen geknüpft werden kann.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Zugriffsmöglichkeit auf die Speichermedien mit verschlüsselten Daten zentral gesteuert und erfasst werden kann.

3. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, dass bei unterschiedlichen Inhalten auf dem Speichermedium die Dateien mit unterschiedlichen Schlüsseln verschlüsselt werden.

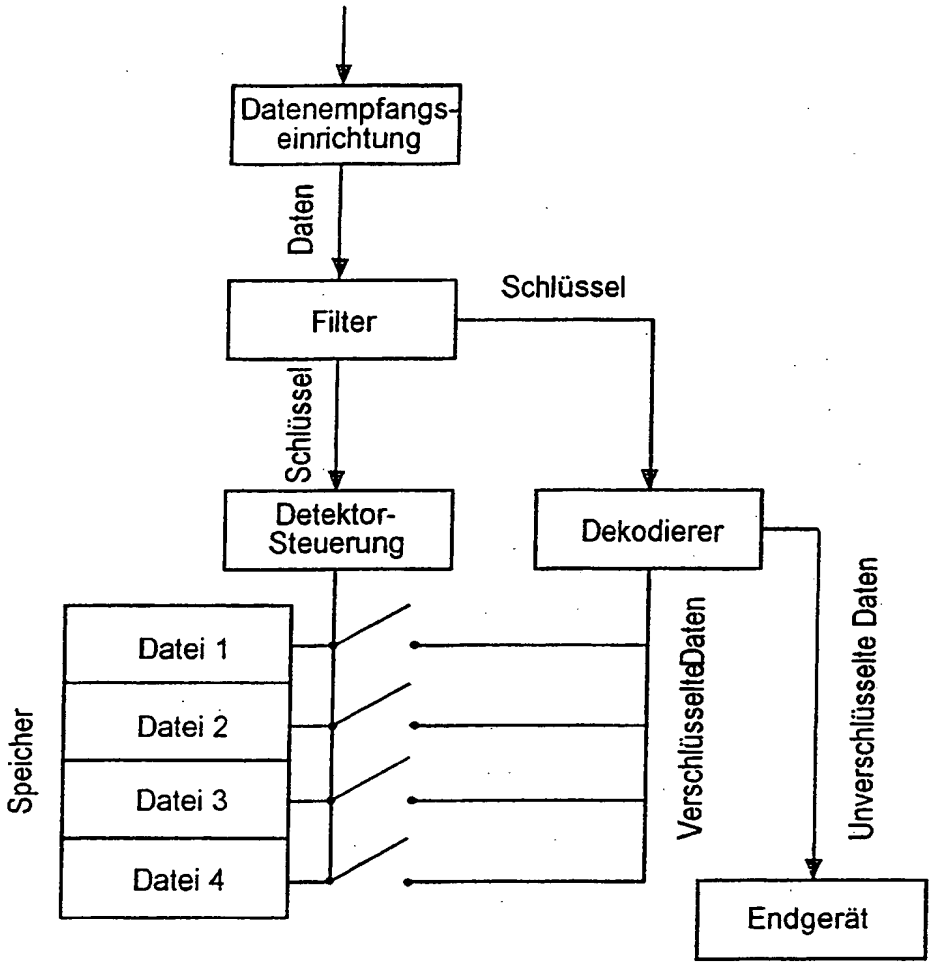

Datenempfangs-einrichtung
Daten
Filter
Schlüssel
Schlüssel
Detektor-Steuerung
Dekodierer
Speicher
Datei 1
Datei 2
Datei 3
Datei 4
Verschlüsselte Daten
Unverschlüsselte Daten
Endgerät

Fig. 1

INTERNATIONAL SEARCH REPORT

Im ational Application No
PCT/EP 00/09428

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 892 825 A (FENG JIE ET AL) 6 April 1999 (1999-04-06) column 3, line 53 -column 8, line 47	1-3
X	PATENT ABSTRACTS OF JAPAN vol. 1997, no. 06, 30 June 1997 (1997-06-30) & JP 09 034841 A (FUJITSU LTD), 7 February 1997 (1997-02-07) abstract	1-3
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 14, 22 December 1999 (1999-12-22) & JP 11 250141 A (NIPPON TELEGR &TELEPH CORP <NTT>), 17 September 1999 (1999-09-17) abstract	1-3

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 February 2001	09/03/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 00/09428

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5892825 A	06-04-1999	AU 5259898 A	22-06-1998
		EP 0974217 A	26-01-2000
		US 6035329 A	07-03-2000
		WO 9824037 A	04-06-1998
		US 5937164 A	10-08-1999
JP 09034841 A	07-02-1997	NONE	
JP 11250141 A	17-09-1999	NONE	

INTERNATIONALER RECHERCHENBERICHT

Im ...tionales Aktenzeichen
PCT/EP 00/09428

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 892 825 A (FENG JIE ET AL) 6. April 1999 (1999-04-06) Spalte 3, Zeile 53 -Spalte 8, Zeile 47	1-3
X	PATENT ABSTRACTS OF JAPAN vol. 1997, no. 06, 30. Juni 1997 (1997-06-30) & JP 09 034841 A (FUJITSU LTD), 7. Februar 1997 (1997-02-07) Zusammenfassung	1-3
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 14, 22. Dezember 1999 (1999-12-22) & JP 11 250141 A (NIPPON TELEGR &TELEPH CORP <NTT>), 17. September 1999 (1999-09-17) Zusammenfassung	1-3

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. Februar 2001	09/03/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Int. ..tionales Aktenzeichen
PCT/EP 00/09428

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5892825 A	06-04-1999	AU 5259898 A	22-06-1998
		EP 0974217 A	26-01-2000
		US 6035329 A	07-03-2000
		WO 9824037 A	04-06-1998
		US 5937164 A	10-08-1999
JP 09034841 A	07-02-1997	KEINE	
JP 11250141 A	17-09-1999	KEINE	